AW

Secure information transmitting process between a user and a computer using a telecommunication network

Patent number: EP0722152
Publication date: 1996-07-17
Inventor: BERNARD ALAIN (FR)
Applicant: JOURNAL TELEPHONE SOC DU (FR)
Classification:
- international: G07C13/00; G09B7/02
- european: G07C13/00; G09B7/02
Application number: EP19960400041 19960108
Priority number(s): FR19950000203 19950110

Also published as:
FR2729260 (A1)
EP0722152 (B1)

Cited documents:
WO9203805

Abstract of **EP0722152**

A user wishing to send confidential information to a remote computer over a normal telephone system receives a card (10) which bears a serial number (20) and also a secret number (24). The secret number is masked with a material of such a type that it's removal is irreversible. The secret number has at least one position blank or occupied by a symbol. In operation the user transmits the serial number from which the computer derives the secret number and blank space position from it's memory or an algorithm. The user then transmits the secret number inserting a number into the blank space to carry the desired information.

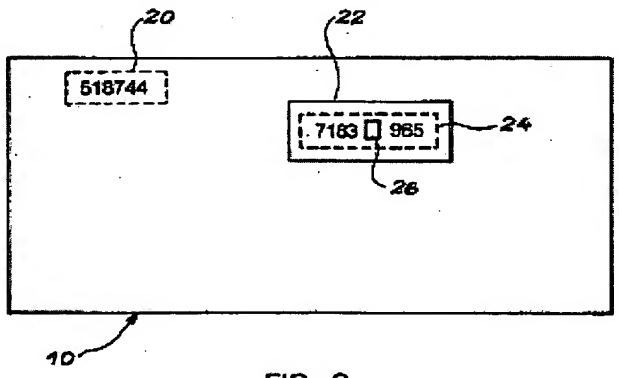

FIG. 2

AW

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 722 152 A1

(12) DEMANDE DE BREVET EUROPEEN

(43) Date de publication:
17.07.1996 Bulletin 1996/29

(51) Int Cl.[6]: **G07C 13/00**, G09B 7/02

(21) Numéro de dépôt: **96400041.8**

(22) Date de dépôt: **08.01.1996**

(84) Etats contractants désignés:
BE DE ES GB IT

(30) Priorité: **10.01.1995 FR 9500203**

(71) Demandeur: **SOCIETE DU JOURNAL TELEPHONE**
92100 Boulogne (FR)

(72) Inventeur: **Bernard, Alain**
F-75015 Paris (FR)

(74) Mandataire: **Dubois-Chabert, Guy et al**
Société de Protection des Inventions
25, rue de Ponthieu
75008 Paris (FR)

(54) Procédé de transmission d'informations protegees entre un utilisateur et un ordinateur par un reseau de telecommunications

(57) L'utilisateur dispose d'un support (10) généralement sous forme de carte, avec numéro de série (20) et numéro secret (24) incomplet. L'utilisateur complète le numéro secret avec un caractère de son choix et envoie le numéro secret complété ainsi que le numéro de série. L'ordinateur (16) retrouve la place du caractère manquant, donc le choix de l'utilisateur.

Application, en particulier, au vote à distance.

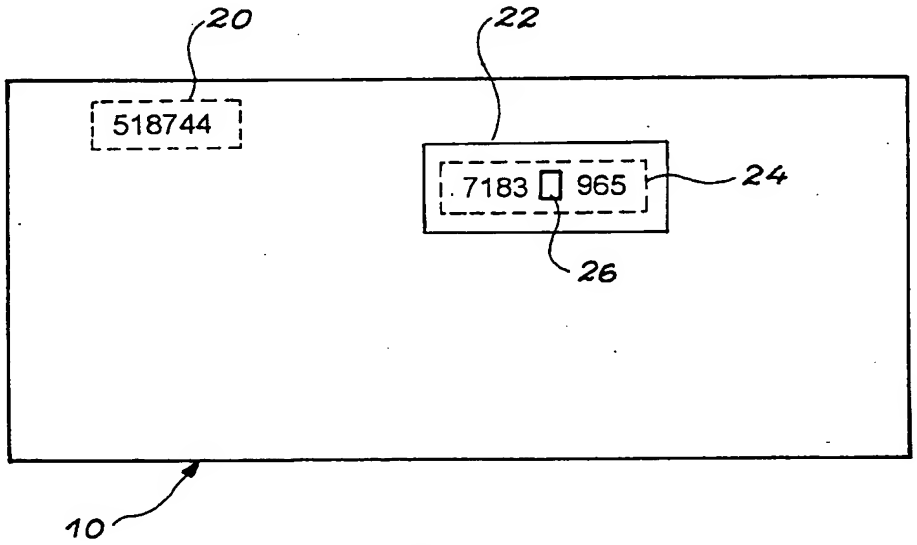

FIG. 2

EP 0 722 152 A1

Description

Domaine technique

La présente invention a pour objet un procédé de transmission d'informations protégées entre un utilisateur et un ordinateur par un réseau de télécommunications. Elle trouve une application dans le vote à distance, le jeu, l'accès à divers services informatiques, etc...

Etat de la technique antérieure

Pour transmettre une information de façon protégée entre un utilisateur et un ordinateur, par un réseau de télécommunications, on connaît diverses techniques, notamment celles qui nécessitent un appareil de chiffrement et celles qui nécessitent un calcul que l'utilisateur effectue, soit manuellement, soit avec une petite calculatrice.

Si elles donnent satistaction a certains egards, ces techniques présentent cependant l'inconvénient de ne pas être adaptées au grand public.

Le but de la présente invention est justement de remédier à cet inconvénient en proposant un procédé accessible à tout un chacun, sans qu'il soit besoin de posséder des connaissances particulières ou de disposer d'un matériel sophistiqué.

Exposé de l'invention

A cette fin, l'invention propose un procédé qui est caractérisé par le fait qu'il comprend les opérations suivantes :

- une autorité délivre à un utilisateur un support sur lequel est inscrit un numéro de série et numéro secret, le numéro secret au moins étant masqué par un moyen à démasquage irréversible, le numéro secret étant composé d'une séquence de caractères dont un au moins est manquant ou remplacé par un symbole spécifique tel que case vide, étoile, carré, etc..., un caractère manquant occupant un emplacement déterminé dans la séquence, le numéro de série de chaque support permettant de retrouver le numéro secret et les emplacements du ou des caractère(s) manquant(s) par une relation secrète connue de l'autorité et de l'ordinateur,
- l'utilisateur démasque le numéro secret de son support, le complète en inscrivant dans le ou les emplacement(s) de caractère(s) manquant (s) un ou des caractère (s) de son choix, ce ou ces caractère (s) constituant l'information à transmettre,
- à l'aide d'un réseau de télécommunications le reliant à un ordinateur, l'utilisateur transmet à cet ordinateur le numéro de série de son support et le numéro secret ainsi complété,
- l'ordinateur, à partir du numéro de série qu'il reçoit et à l'aide de ladite relation qu'il connaît, retrouve le numéro secret associé au numéro de série, vérifie que la séquence secrète qu'il a reçue a bien été émise par le titulaire du support portant le numéro de série reçu, détermine le ou les emplacement(s) dans le numéro secret du (des) caractère (s) manquant (s), lit le ou les caractère(s) figurant dans ce ou ces emplacement(s), en déduit l'information transmise, et agit en fonction de cette information.

L'action finale entreprise par l'ordinateur peut être un enregistrement dans une mémoire, une comptabilisation, une autorisation d'accès, etc...

De préférence, le numéro de série et/ou le numéro secret sont des séquences de caractères littéraux et/ou numériques compatibles avec les caractéristiques du terminal dont dispose l'utilisateur.

De préférence encore, le moyen de masquage irréversible est un film à gratter.

De préférence encore, le caractère manquant est un chiffre compris entre 0 et 9. Dans ce cas, l'information représentée par le chiffre choisi correspond à une entité prise parmi 10 entités.

Le chiffre compris entre 0 et 9 peut désigner une personne parmi 10, l'information transmise étant alors un vote. L'une des applications privilégiée de l'invention est donc le vote à distance. Dans ce cas, le support prend la forme d'un bulletin qui est distribué à chaque électeur après vérification de sa carte électorale. Chaque électeur peut alors etre identifié par le numéro de série du bulletin qui lui est attribué. Dans cette application, l'autorité est un organisme habilité à organiser des élections.

Brève description des dessins

- la figure 1 représente schématiquement un réseau de télécommunications pouvant être utilisé pour la mise en oeuvre du procédé de l'invention ;
- la figure 2 montre un exemple de support sous forme de carte.

Description détaillée d'un mode de réalisation

Conformément à l'exemple de la figure 1, un utilisateur qui a reçu une carte 10, veut transmettre une information en utilisant un téléphone à touches 12 en utilisant un réseau téléphonique 14 le reliant à un ordinateur 16.

Dans l'exemple qui va être décrit, l'utilisateur cherche à transmettre un chiffre compris entre 0 et 9. Comme représenté sur la figure 2, l'utilisateur a reçu une carte 10 comprenant un numéro de série 20 ce numéro (518744 dans l'exemple illustré) et un nombre secret assez long 24 (7183 965 dans l'exemple illustré) protégé contre la lecture par un film 22 susceptible d'être gratté ou par une enveloppe.

Ce nombre secret comporte une série de caractères mais l'un d'eux au moins, est par exemple, une case

blanche 26.

A partir du numéro de série 20, l'ordinateur central 16 peut trouver le nombre secret 24 et la position de la case blanche 26. Les données nécessaires à ces opérations ont, par exemple, été stockées dans une table, ou peuvent être déduites du numéro de série 20 par un algorithme.

L'utilisateur fait alors son choix, matérialisé par un chiffre compris entre 0 et 9. Il gratte la protection 22 du numéro secret 24 et inscrit son choix dans la case blanche 26 ou à la place du symbole spécifique. Ensuite, il appelle l'ordinateur et tape le numéro de série 20, puis la totalité des chiffres du numéro secret 24, y compris le chiffre correspondant à son choix.

Le serveur vocal et les divers moyens qui sont dans la chaîne de télécommunications ne peuvent savoir quel est l'emplacement de la séquence qui correspond au choix de l'utilisateur. Par contre, l'ordinateur est capable de trouver, par le numéro de série, le chiffre qui a été ajouté à la séquence secrète. Il peut aussi vérifier que la séquence reçue a bien été émise par le possesseur de la carte identifiée par son numéro de série.

Dans une variante de l'invention, le numéro de série 20 est également protégé par une enveloppe ou par un film de grattage.

Revendications

1. Procédé de transmission d'informations protégées entre un utilisateur et un ordinateur par un réseau de télécommunications, caractérisé par le fait qu'il comprend les opérations suivantes :

   - une autorité délivre à un utilisateur un support (10) sur lequel est inscrit un numéro de série (20) et numéro secret (24), le numéro secret (24) au moins étant masqué par un moyen à démasquage irréversible (22), le numéro secret (24) étant composé d'une séquence de caractères dont un au moins (26) est manquant ou remplacé par un symbole spécifique, un caractère manquant (26) occupant un emplacement déterminé dans la séquence (24), le numéro de série (20) de chaque support (10) permettant de retrouver le numéro secret (24) et les emplacements (26) du ou des caractère(s) manquant(s) par une relation secrète connue de l'autorité et de l'ordinateur (16),
   - l'utilisateur démasque le numéro secret (24) de son support (10), le complète en inscrivant dans le ou les emplacement(s) (26) où un caractère est manquant un ou des caractère(s) de son choix, ce ou ces caractère(s) constituant l'information à transmettre,
   - à l'aide d'un réseau de télécommunications (14) le reliant à un ordinateur (16), l'utilisateur transmet à cet ordinateur (16) le numéro de série (20) de son support (10) et le numéro secret (24) ainsi complété,
   - l'ordinateur (16), à partir du numéro de série (20) qu'il reçoit et à l'aide de ladite relation qu'il connaît, retrouve le numéro secret (24) associé au numéro de série (20), vérifie que la séquence secrète (24) qu'il a reçue a bien été émise par le titulaire du support (10) portant le numéro de série reçu (20), détermine le ou les emplacement(s) (26) dans le numéro secret (24) du (des) caractère(s) manquant(s), lit le ou les caractère(s) figurant dans ce ou ces emplacement(s) (26), en déduit l'information transmise, et agit en fonction de cette information.

2. Procédé selon la revendication 1, caractérisé par le fait que l'utilisateur transmet à l'ordinateur (16) le numéro de série (20) et le numéro secret complété (24) en utilisant le réseau téléphonique (14).

3. Procédé selon la revendication 1, caractérisé par le fait que le numéro de série (20) et/ou le numéro secret (24) sont des séquences de caractères littéraux et/ou numériques.

4. Procédé selon la revendication 1, caractérisé par le fait que le moyen de masquage irréversible (22) est un film à gratter.

5. Procédé selon la revendication 1, caractérisé par le fait que le caractère manquant (26) est un chiffre compris entre 0 et 9.

6. Procédé selon la revendica tion 5, caractérisé par le fait que l'information représentée par le chiffre choisi compris entre 0 et 9 correspond à une entité prise parmi 10 entités.

7. Procédé selon la revendication 6, caractérisé par le fait que le chiffre choisi compris entre 0 et 9 désigne une personne parmi 10, l'information transmise étant alors un vote.

8. Procédé selon l'une quelconque des revendications 1 à 7, caractérisé par le fait qu'on utilise des supports genre cartes ou bulletins.

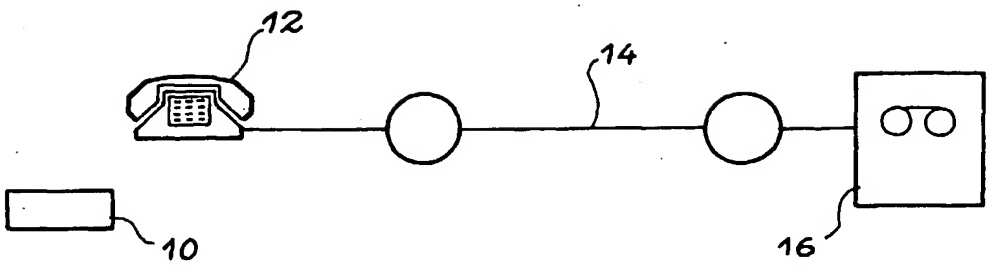

FIG. 1

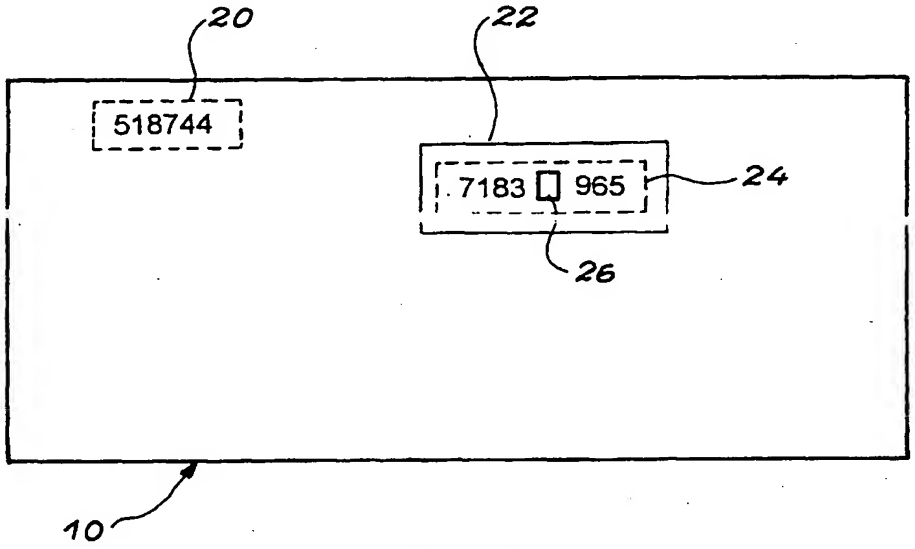

FIG. 2

Office européen des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numero de la demande
EP 96 40 0041

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (Int.Cl.6)
A	WO-A-92 03805 (TECNOMEN) * page 10, ligne 4 - page 14, ligne 29 * -----	1	G07C13/00 G09B7/02

DOMAINES TECHNIQUES RECHERCHES (Int.Cl.6)

G07C
G09B

Le présent rapport a été établi pour toutes les revendications

Lieu de la recherche	Date d'achèvement de la recherche	Examinateur
LA HAYE	25 Avril 1996	Taccoen, J-F

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C02)